BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/721,942	11/27/2000	Ulf Mattsson	0104-0310P	4284

2292 7590 07/02/2004

BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 07/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/721,942	MATTSSON ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-7 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-7 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 27 November 2000 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2/6/2001.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-7 have been examined.

Specification

2. The abstract is objected to because of the following informalities: it includes legal terms such as "means" and "said". Appropriate correction is required.

3. Claims 1 and 7 are objected to because of the following informalities: insert "in" between "included" and "said" in the line next to the last line of each claim. Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1, 5 and 7 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a. Regarding claims 1 and 7, it recites the limitation "said restricted character set" in (lines 12 and 14 of claim 1, line 12 of claim 7). There is insufficient antecedent basis for this limitation in the claim.

b. Regarding claim 5, it recites the limitation "the varying integer value" in the second line. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lyson et al. (6,327,595) in view of Deldo et al. (6,389,414) and Febvre (5,333,197). Regarding claim 1, which is representative of claim 7, Lyson discloses a method for encryption of a data element in a relational database, wherein said database comprises a plurality of data elements of at least one type, and each data element comprises a string of at least one character (see Abstract, fig. 1) comprising the steps of:

reading the type of a data element which is to be encrypted (fig. 2, steps 42-44); and

interpreting the data type to retrieve an associated symmetric key and encrypting the data element using the symmetric key (fig. 2, steps 46-50).

Lyson does not disclose the steps of interpreting said data type in order to form a restricting character set for the data type. Deldo discloses a method for validating data to be stored in a relational database comprising the steps of interpreting the data type of the data in order to form a restricting character set for the data type and using the restricting character set to ensure that the data entered meets the criteria defined by the

data type (col. 1, lines 33-39). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Lyson to include the steps of interpreting the data type of the data in order to form a restricting character set for the data type and using the restricting character set to ensure that the data entered meets the criteria defined by the data type, as taught by Deldo. The motivation for doing so would have been to maintain the validity of the database.

Lyson does not disclose the step of encrypting each character of said data element into an encrypted character using said restricting character set to control the encryption process to only create encrypted characters included in said restricting character set. Febvre discloses an encryption method comprising the step of encrypting each character into an encrypted character using a restricting character set to control the encryption process to only create encrypted characters included in said restricting character set (col. 1, line 59-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Lyson to include the step of encrypting each character of said data element into an encrypted character using said restricting character set to control the encryption process to only create encrypted characters included in said restricting character set, as taught by Febvre, in order to prevent the encoder from generating undesired characters.

8. Claims 2-4 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lyson, Deldo and Febvre as applied to claim 1 above, and further in view of Schneier ("Applied Cryptography").

a. Regarding claim 2, Lyson, Deldo and Febvre do not disclose the step of arranging one or more character sets in a pattern for a data type. Schneier discloses an encryption scheme called one-time pad in which a character set is arranged in a pattern for a data type (Section 1.5, page 15, "Believe it or not ... and the one-time pad key character."). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Lyson, Deldo and Febvre to use the one-time pad encryption scheme in which a character set is arranged in a pattern for a data type, as taught by Schneier, because it is a perfect encryption scheme.

b. Regarding claim 3, Lyson, Deldo and Febvre do not disclose that the encryption results in a data element having the same number of characters as the unencrypted data element. Schneier discloses an encryption scheme called one-time pad in which the encryption results in the encrypted data having the same number of characters as the unencrypted data (page 15). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Lyson, Deldo and Febvre to use the one-time pad encryption scheme in which the encryption results in the encrypted data having the same number of characters as the unencrypted data, as taught by Schneier. Please refer to the motivation for using the one-time pad encryption scheme discussed in claim 2.

c. Regarding claim 4, Lyson, Deldo and Febvre do not disclose the steps of converting each character to an index value and adding a varying value to each index value before encryption. Schneier discloses an encryption scheme including the steps of converting each character to an index value and adding a varying value to each index

value before encryption (page 15). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Lyson, Deldo and Febvre to use the one-time pad encryption scheme including the steps of converting each character to an index value and adding a varying value to each index value before encryption. Please refer to the motivation for using the one-time pad encryption scheme discussed in claim 2.

d. Regarding claim 6, Lyson, Deldo and Febvre do not disclose using the DES algorithm in stream cipher mode. Schneier discloses using the DES algorithm in CFB mode of operation, which meets the limitation of DES algorithm in stream cipher mode (Section 12.2, page 277, see Modes of DES). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Lyson, Deldo and Febvre to use the DES algorithm in stream cipher mode. The motivation for doing so would have been that the 8-bit CFB is generally the mode of choice for encrypting stream of characters when each character has to be treated individually (Section 9.11, page 210).

9. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lyson, Deldo, Febvre and Schneier as applied to claim 4 above, and further in view of Marshall et al. (4,866,707). Lyson, Deldo, Febvre and Schneier (Section 1.5) do not disclose adding adjacent index values pairwise from the left to the right using said initial value when adding the leftmost character. Schneier, in Section 9.3, discloses a cipher block chaining (CBC) mode in which adjacent blocks are XORed pairwise from the left to the

right using an initialization vector with the leftmost unit (page 194, fig. 9.3 and "Prevent this by encrypting ... use some random bits from someplace."); the teaching of Schneier reads on the adding step of the claim. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Lyson, Deldo, Febvre and Schneier (Section 1.5) to include the step of adding adjacent index values pairwise from the left to the right using said initial value when adding the leftmost character, as taught by Schneier (Section 9.3). The motivation for doing so would have been that the ciphertext block is dependent not just on the plaintext block that generated it but on all the previous plaintext blocks (page 193).

Lyson, Deldo, Febvre and Schneier do not disclose creating an initial value by hashing the encryption key. Marshall discloses a CBC encryption technique including the step of creating an initialization vector by encrypting a message key (col. 9, lines 13-19); the teaching of Marshall reads on the creating step of the claim. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Lyson, Deldo, Febvre and Schneier to include the step of creating an initial value by hashing the encryption key, as taught by Marshall. The motivation for doing so would have been that the same message being sent a second time would be encrypted under a different key, so an outsider would not be able to gain much assistance from the repetition in trying to breach the encryption (col. 9, lines 27-33).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 703-306-5617. The examiner can normally be reached on Mon - Fri: 9:00 am - 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
6/24/2004

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100